HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 10971806-3

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): Josh Hogan

Confirmation No.: 2220

Application No.: 09/783,112

Examiner: Thomas A. Gyorfi

Filing Date: February 14, 2001

Group Art Unit: 2135

Title: METHOD AND APPARATUS FOR PERFORMING DATA ENCRYPTION AND ERROR CODE CORRECTION

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on 12-2-2006.

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) $500.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

☒ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

☐ 1st Month $120	☐ 2nd Month $450	☐ 3rd Month $1020	☐ 4th Month $1590

☐ The extension fee has already been filed in this application.

☒ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of $ 500. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees.

Respectfully submitted,

Josh Hogan

By: /Hugh Gortler #33,890/

Hugh P. Gortler

Attorney/Agent for Applicant(s)

Reg No. : 33,890

Date : 1/12/2007

Telephone : (949) 454-0898

I hereby certify that this document is being transmitted to the Patent and Trademark Office via eletronic filing.

Date of Transmission: 1/12/2007

Patent
Docket No. 10971806-3

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

APPEAL NO. _____

In re Application of:
Josh Hogan

Serial No. 09/783,112
Filed: February 14, 2001

Confirmation No. 2220
Group Art Unit: 2135
Examiner Thomas A. Gyorfi

For: METHOD AND APPARATUS FOR PERFORMING DATA ENCRYPTION AND ERROR CODE CORRECTION

APPEAL BRIEF

Hugh P. Gortler, Esq.

Hewlett-Packard Company
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

(949) 454-0898

INDEX

1. REAL PARTY IN INTEREST

The real party in interest is the assignee, Hewlett-Packard Development Company.

2. RELATED APPEALS AND INTERFERENCES

No appeals or interferences are known to have a bearing on the Board's decision in the pending appeal.

3. STATUS OF CLAIMS

Claims 26-28 are pending in this application.

Claim 26 is allowed.

Claims 27-28 are rejected.

The rejections of claims 27-28 are being appealed.

4. STATUS OF AMENDMENTS

A final office action dated March 6, 2006 indicated that claims 26-28 were allowed, but claims 1 and 10 were rejected. In response to the final action, claims 1 and 10 were cancelled. A non-final office action was issued on August 3, 2006, and it withdrew the allowability of claims 27-28. A response was filed on Nov. 29, 2006 to address one of the issues raised in the August 3rd action (claim 27 was amended). A notice of appeal was filed subsequent to the response.

The claims are listed in appendix A. The amendment to claim 27 is presented in bold italics.

5. SUMMARY OF CLAIMED SUBJECT MATTER

The present invention addresses the problem of sending ECC-encoded blocks to a computer bus that is not secure. In a DVD drive, for instance, it might be desirable to send certain ECC-encoded blocks from the drive to a host computer for ECC-decoding. The host computer could perform more flexible error correction methods than the drive. For example, the DVD drive could execute a default routine that is fast and that could correct a large majority of errors. Errors that could not be corrected by the default routine would be corrected by the host processor, using a more complex routine, such as a "heroic data recovery" routine.

The ECC blocks would be sent to the host computer's processor via a computer bus. However, if the computer bus is not secure, the unencrypted data in the blocks would be vulnerable to theft and unauthorized copying.

The ECC blocks could be encrypted before being sent to the computer bus. However, the integrity of the code words would be destroyed by encryption.

The inventor has found that a specific type of encryption – XOR encryption – does not destroy the integrity of the code words. The ECC blocks can be XOR-encrypted in the drive, and sent to a host computer for error code correction. Moreover, the XOR encryption allows the host to perform the error code correction on the encrypted ECC blocks, without having to decrypt the ECC blocks. Error-corrected data, still encrypted, could then be sent downstream to an authorized device (e.g., an authorized DVD decoder card) for decryption.

Claim 27 recites a drive comprising a reader, and a controller for performing a bitwise XOR of an encryption mask and a block of ECC-encoded data provided

by the reader. A product of the bitwise XOR is an encrypted block.

Claim 28 recites a data controller comprising a processor for performing a bitwise XOR of an encryption mask and a block of ECC-encoded data. A product of the bitwise XOR is an encrypted block.

Figure 1 of the application provides an example of the drive of claim 27 and the data controller of claim 28. A DVD drive 16 includes a reader 18 and the data controller 20. According to page 5, lines 11+, the reader 18 is operable to read RS-PC blocks stored on a DVD disc. According to page 6, lines 8+, a bitwise XOR of an encryption mask and a block of ECC-encoded data is then performed.

An RS-PC block, which is a type of ECC block, is illustrated in Figure 4 and described at page 7, line 29 to page 8, line 11. An example of bitwise XOR encryption of a line 501 of an RS-PC block and a line 502 of an encryption mask is illustrated in Figure 5 and described at page 8, lines 12+. According to page 11, lines 1+, the RS-PC block may be fully or partially encrypted.

According to page 6, lines 13+, the XOR-encrypted ECC block can be placed on a computer bus 12, where it is sent to a computer processor 14 for ECC decoding. The XOR-encryption provides protection against theft and unauthorized copying, even if the bus 12 is not secure. The XOR encryption does not destroy the integrity of the ECC code words. Further, the XOR encryption allows the processor 14 to perform the ECC-decoding on the encrypted ECC block without performing decryption. Advantageously, the ECC-decoding can be performed on the encrypted ECC block, and the decryption can be performed downstream by a trusted entity (page 5, lines 2-3, and page 7, lines 11-22).

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

a. Base claim 27 is rejected under 35 USC §103(a) as being unpatentable over Menzees in view of Chuang.

b. Base claim 28 is rejected under 35 USC §102(a) as being anticipated by Menzees.

c. Base claim 27 is rejected under 35 USC §112, second paragraph as being indefinite.

7. ARGUMENTS

I

REJECTION OF BASE CLAIM 27 UNDER 35 USC §103 AS BEING UNPATENTABLE OVER MENZEES IN VIEW OF CHUANG

The drive of claim 27 offer solutions to the following problem: how to send ECC blocks to a computer over an insecure bus without (1) destroying the integrity of the ECC code words; and (2) not leaving the ECC blocks vulnerable to theft and unauthorized copying. Menzees and Chuang, alone and in combination, do not teach or suggest a solution to this problem.

Chuang is not relevant to this problem. Chuang is concerned with increasing the throughput from an optical drive to a computer data bus (col. 3, lines 43-45). Chuang purportedly increases the throughput by modifying error detection and correction.

Chuang does not teach or suggest that ECC coding is performed outside of the optical drive. Chuang clearly discloses that ECC coding is necessarily

performed within the optical drive. See col. 1, lines 60+ (a variety of operations "must be" performed on data read from a CD disk before the data can be provided to the data buses of a host computer, including error correction).

Chuang does not teach or suggest a bitwise XOR of an encryption mask and a block of ECC-encoded data. Chuang describes XOR operations in connection with error check division (col. 3, lines 19-30), which is part of error detection.

Chuang does not even teach or suggest encrypting ECC blocks.

Menzees describes XOR encryption on data strings. However, Menzees does not teach or suggest XOR encryption of ECC blocks.

Thus, the combined teachings of Menzees and Chuang do not produce a drive having all of the features of claim 27.

Furthermore, the office action does not find motivation in the prior art for combining the teachings of Menzees and Chuang. The office action states that the motivation for combining the teachings of Menzees and Chuang would be to give Chuang's controller "a source of operands without which it could not perform its function." The office action does not explain why this is so, and it seems to ignore the fact that Chuang's drive can already perform its necessary functions of ECC detection and correction. Neither Chuang nor Menzees suggests that encryption of ECC blocks is necessary.

Moreover, the motivation is not found in the prior art. It is an unsubstantiated allegation by the examiner (the allegation has been challenged above). Thus far, the record provides no evidence of motivation to perform XOR encryption of ECC blocks.

The examiner made a similar rejection in the office action dated May 25, 2006, except that he relied on Sako instead of Chuang, and Schneier (Applied Cryptography, 2nd ed., 1996) instead of Menzees. However, the new grounds of rejection does not remove Schneier from the prior art.

Schneier teaches away from the use of XOR encryption. On page 14, Schneier states XOR encryption is "an embarrassment" and is "trivial to break Schneier does not disclose the advantages of XOR encryption: XOR encryption – does not destroy the integrity of the code words in an ECC block, and XOR encryption allows a host to perform the error code correction without having to decrypt the block. Menzees does not disclose these advantages either.

Out of the myriad of available encryption algorithms, the examiner says it is obvious to use XOR encryption, even though Schneier teaches away from its use, and Menzees and Chuang offer no advantages. Only the applicant gives reasons for using XOR encryption. Thus, the examiner is engaging in hindsight reconstruction, using applicants' structure as a template and selecting elements from the cited documents to fill the gaps. However, such hindsight reconstruction does not provide a legal basis for a '103 rejection.

II
REJECTION OF BASE CLAIM 28 UNDER 35 USC §102 AS BEING ANTCIPATED BY MENZEES

The processor of claim 28 offers a solution to the following problem: how to send ECC blocks to a computer over an insecure bus without (1) destroying the integrity of the ECC code words; and (2) not leaving the ECC blocks vulnerable to theft and unauthorized copying.

Menzees does not address this problem. Menzees simply discloses XOR encryption of binary strings of length six.

The examiner "notes" that ECC-encoded data is merely binary data, but this is tantamount to saying the MPEP is merely a group of letters. An ECC block has a specific structure. Consider the RS-PC block 400 illustrated in Figure 4. The RS-PC block has a header 401, user data 405 and error correction codes 403 and 404. The codes 403 and 404 provide a specific function: correcting errors in the user data. An ECC block is not merely data.

Menzees does not teach or suggest XOR encryption of ECC code words. For this reason alone, the '102 rejection of claim 28 should be withdrawn. The '102 rejection should be withdrawn for the additional reason that Menzees does not disclose data controller comprising a processor.

The examiner cites MPEP 2131.02 [*sic*], and states Menzees anticipates the genus of claim 28 and therefore anticipates claim 28, which is the species of the genus. The examiner appears to have it backwards. MPEP 2131.02 states "A generic claim cannot be allowed to an applicant if the prior art discloses a species

falling within the claimed genus." Thus, if Menzees anticipates claim 28, it also anticipates a claim that is broader than claim 28. However, Claim 28 is a base claim, it does not depend from a broader claim. Moreover, Menzees does not anticipate claim 28 since it does not set forth each and every element as set forth in claim 28, either expressly or inherently.

III
REJECTION OF BASE CLAIM 27 UNDER 35 USC §112, SECOND PARAGARPH, AS BEING INDEFINITE

Two separate reasons for indefiniteness were indicated in the office action dated August 3, 2006. The first reason had to do with the lack of inter-relationship between reader and controller. This reason has been rendered moot by the amendment filed Nov. 29, 2006. Claim 27 was amended to recite a controller for performing a bitwise XOR of an encryption mask and a block of ECC-encoded data provided by the reader (the underlined portion was added in the amendment). Thus, the first reason for indefiniteness has been rendered moot.

As for the second reason for indefiniteness, the office action indicates that the limitations of claim 27 are not sufficient to perform the functions of a drive. This '112 rejection based on this second reason is traversed.

Section 112 does not require a claim 27 to recite a fully functional drive. "The purpose of claims is not to explain the technology or how it works, but to state the legal boundaries of the patent grant." S3 Inc. v. nVIDIA Corp., 259 F.3d 1364, 1367 (Fed. Cir. 2001). "The requirement that the claims 'particularly point[] out and distinctly claim[]' the invention is met when a person experienced in the field of

the invention would understand the scope of the subject matter that is patented when the claim is read in conjunction with the rest of the specification. If the claims when read in light of the specification reasonably apprise those skilled in the art of the scope of the invention, §112 demands no more." Miles Laboratories, Inc. v. Shandon, 997 F.2d 870, 875, 27 USPQ2d 1123, 1126 (Fed. Cir. 1993) cited in S3 Inc. v. nVIDIA Corp., 259 F.3d 1364, 1367 (Fed. Cir. 2001).

Claim 27 recites a drive that performs XOR encryption of an encryption mask and a block of ECC-encoded data. The office action does not indicate that this feature is unclear to a person skilled in the art, and section 112 demands no more. Therefore, the '112 rejection of claim 27 should be withdrawn.

For the reasons above, the rejections of claims 27-28 should be withdrawn. The Honorable Board of Patent Appeals and Interferences is respectfully requested to reverse these rejections.

Respectfully submitted,

/Hugh Gortler #33,890/
Hugh P. Gortler, Esq.
Registration No. 33, 890

Hewlett-Packard Company
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

(949) 454-0898

Date: January 12, 2007

8. CLAIMS APPENDIX

26. (Previously presented) A system comprising:

a computer bus;

a host processor programmed to perform error code correction; and

a drive for providing an encryption mask, the drive performing a bitwise XOR of an encryption mask and a block of ECC-encoded data, a product of the bitwise XOR being an encrypted block; the drive providing the encrypted block to the computer bus, whereby an encrypted block can be sent to the host processor via the computer bus for error code correction.

27. (Previously presented) A drive comprising:

a reader; and

a controller for performing a bitwise XOR of an encryption mask and a block of ECC-encoded data ***provided by the reader***, a product of the bitwise XOR being an encrypted block.

28. (Previously presented) A data controller comprising a processor for performing a bitwise XOR of an encryption mask and a block of ECC-encoded data, a product of the bitwise XOR being an encrypted block.

9. EVIDENCE APPENDIX

None

10. RELATED PROCEEDINGS APPENDIX

None